Server Alarms

• Server Components Alarms, on page 1

Server Components Alarms

Following table shows the description of the supported alarms for servers.

Name	MO	Severity	Explanation	Recommended Action
BladeMigrationDetected	compute.Blade	Critical	This alarm occurs when a server has been detected in a slot different than the one it was discovered in.	1. Reacknowledge the server in the current slot. 2. If the issue persists, remove the server from the current slot and reinsert it in the correct slot. 3. Reacknowledge the server in the correct slot. 4. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
PhysicalMissing	compute.Physical	Critical	This alarm occurs when a server has been removed from the slot it was discovered in.	1. Make sure a server is inserted in the slot. 2. Check the Power-On-Self-Test (POST) results for the server. 3. Check the power state of the server. 4. If the server is off, turn the server on. 5. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
PhysicalWillBoot	compute.Physical	Critical	The UCS Will Boot is a cursory check to ensure that the blade is configured properly to allow the BIOS to proceed. This alarm indicates that a critical Will boot error is encountered on the server. This error occurs when the CPU and DIMM configuration check fails.	1. Verify that the DIMMs are installed in a supported configuration. 2. Verify that an adapter and CPU are installed. 3. Download the System Event Logs file from the GUI by clicking **Servers>Server Name>... >System>Download System Event Log** 4. Review the SEL statistics on the DIMM to determine which threshold was crossed. 5. Create a `show tech-support file` and contact Cisco TAC to see if the DIMM needs replacement.
BoardTemperatureWarning	compute.Board	Warning	The motherboard has a warning temperature threshold condition.	1. Review the product specifications to determine the operating temperature range. 2. Power off unused blade servers and rack servers. 3. Verify that the server fans are working properly. 4. Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat. 5. Set the power profiling, power priority of the server, and the power restore state of the system through server Power Policy. 6. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
BoardTemperatureCritical	compute.Board	Critical	The motherboard has a critical temperature threshold condition.	1. Verify that the server fans are working properly. 2. Wait for 24 hours to see if the problem resolves itself. 3. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
BoardVoltageWarning	compute.Board	Warning	The motherboard has a warning voltage threshold condition.	1. Ensure that the motherboard is supplied with the required input voltage as per the product specifications. 2. Create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
BoardVoltageCritical	compute.Board	Critical	The motherboard has a critical voltage threshold condition.	1. Ensure that the motherboard is supplied with the required input voltage as per the product specifications. 2. Create a `show tech-support` file and contact Cisco TAC.
BoardPower	compute.Board	Critical	The motherboard has a critical power problem. This occurs when the motherboard power consumption exceeds certain threshold limits. At that time the power usage sensors on a server detect a problem.	1. Ensure that the motherboard is supplied with the required input voltage as per the product specifications. 2. Create a `show tech-support` file and contact Cisco TAC to see if the motherboard needs replacement.
ServerAdapterUnitDeprecated	compute.Physical	Critical	One or more adapters connected to the server are deprecated, or are not supported in the current Intersight release.	1. Verify that only the supported adapters are installed on the server. 2. If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
RackUnitHealthWarning	compute.RackUnit	Warning	The server's health state has reached the warning threshold.	1. Read fault summary and determine course of action. 2. If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
RackUnitHealthCritical	compute.RackUnit	Critical	The server's health state has reached the critical threshold.	1. Read fault summary and determine course of action. 2. If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
PciNodeInsertedPowerOnRequired	compute.Blade	Warning	This alarm occurs if PCIe node is inserted when the compute node is in powered off state.	1. After inserting the PCIe node, power on the PCIe node's paired compute node. 2. After the paired compute node is completely powered on, rediscover the PCIe node.

Name	MO	Severity	Explanation	Recommended Action
PciNodeRemovedPowerOnRequired	compute.Blade	Warning	This alarm occurs if PCIe node is removed when the compute node is in powered off state.	After removing the PCIe node, power on the PCIe node's paired compute node.
PciNodeInsertedPowerCycleRequired	compute.Blade	Warning	This alarm occurs if PCIe node is inserted when the compute node is in powered on state.	1. Power down the paired compute down. 2. After the paired compute node is completely powered off. Remove the PCIe node. 3. Before re-inserting a PCIe node, make sure that its paired compute node is powered off. 4. After the paired compute node has completely powered off, insert the PCIe node. Insert the PCIe node. 5. Power on the PCIe node's paired compute node. 6. After the paired compute node is completely powered on, rediscover the PCIe node.
PciNodeRemovedPowerCycleRequired	compute.Blade	Warning	This alarm occurs if PCIe node is removed when the compute node is in powered on state.	1. Power down the paired compute down. 2. After the paired compute node is completely powered off. Remove the PCIe node. 3. Power on the PCIe node's paired compute node. 4. After the paired compute node is completely powered on, rediscover the PCIe node.
PciNodeUnsupported	compute.Blade	Warning	Unsupported PCIe node detected. PCIe node will remain powered off.	1. Verify that the PCIe node is running the recommended firmware version by checking here **Servers>Server Name>Inventory>GPUs >PCIe-Node-GPU Name>General** 2. Verify that the paired compute node is running the recommended firmware version by checking here **Servers>Server Name>General** 3. If the firmware versions are compatible, create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
PciNodeUnidentified	compute.Blade	Warning	Unidentified PCIe node detected. PCIe node will remain powered off.	1. Verify that the inserted PCIe node is running the recommended firmware version here **Servers>Server Name>Inventory>** **GPUs>PCIe-Node-GPU Name>General** 2. If the firmware is supported, create a `show tech-support` file and contact Cisco TAC.
HostEthInterfaceDown	adapter.HostEthInterface	Critical	The uplink interface is shut down, or a transient error caused the vNIC to fail.	1. If an associated port is disabled, enable the port. 2. Reacknowledge the server with the Ethernet adapter that has the failed link. 3. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
HostEthInterfaceStandByActive	adapter.HostEthInterface	Warning	The preferred path for the failover enabled vNIC is down and hence the secondary path is currently active.	1. Update the configuration of the port or port channel to include the primary VLAN. 2. If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
HostFcInterfaceDown	adapter.HostFcInterface	Critical	The uplink interface is shut down, or a transient error caused the vHBA to fail.	1. If an associated port is disabled, enable the port. 2. Reacknowledge the server with the Fibre Channel adapter that has the failed link. 3. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
NotReachable	adapter.Unit	Warning	Adapter is not reachable or the connectivity is not discovered from the Fabric Interconnects or FEX.	1. Check if the corresponding Input/Output module is inserted in the chassis. 2. Check if CIMC/BIOS are running recommended firmware version. 3. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
CardTemperatureWarning	graphics.Card	Warning	The GPU has a warning temperature threshold condition.	1. Verify that the server fans are working properly. 2. Wait for 24 hours to see if the problem resolves itself. 3. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
CardTemperatureCritical	graphics.Card	Critical	The GPU has a critical temperature threshold condition.	1. Verify that the server fans are working properly. 2. Wait for 24 hours to see if the problem resolves itself. 3. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
UnitTemperatureWarning	memory.UnitPSU	Warning	The memory unit has a warning temperature threshold condition.	1. Verify that the server fans are working properly. 2. Wait for 24 hours to see if the problem resolves itself. 3. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
UnitTemperatureCritical	memory.Unit	Critical	The memory unit has a critical temperature threshold condition.	1. Verify that the server fans are working properly. 2. Wait for 24 hours to see if the problem resolves itself. 3. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
UnitUncorrectableError	memory.Unit	Critical	The memory unit has encountered an uncorrectable ECC error.	1. Monitor the error statistics of the degraded DIMM. 2. Create a `show tech-support` file and contact Cisco TAC to see if the inoperable DIMM needs a replacement.
UnitBankError	memory.Unit	Warning	The memory unit has encountered a Bank Virtual lock step (VLS) error.	1. Restart the host so that the DIMM gets auto-repaired. 2. If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
UnitRankError	memory.Unit	Warning	The memory unit has encountered a Rank Virtual lock step (VLS) error.	1. Restart the host so that the DIMM gets auto-repaired. 2. If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
UnitInvalidPopulation	memory.Unit	Critical	The DIMM slot has been invalidly populated.	1. Reseat the DIMM into the correct slot. 2. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
UnitRasModeError	memory.Unit	Critical	The memory unit has encountered a RAS Mode error.	1. Reboot the server. 2. If the issue persists, verify that the DIMMs are installed in a supported configuration. 3. Reseat the DIMM. 4. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC to see if the DIMM needs a replacement.
UnitMismatchError	memory.Unit	Critical	A memory mismatch has been detected on this memory unit.	Create a `show tech-support file` and contact Cisco TAC to see if the mismatched DIMM needs a replacement.
UnitSpdError	memory.Unit	Critical	The memory unit has encountered a SPD error.	Create a `show tech-support file` and contact Cisco TAC to see if the faulty component of the DIMM needs a replacement.
UnitBistError	memory.Unit	Critical	The memory unit has encountered a BIST error.	Create a `show tech-support file` and contact Cisco TAC to see if the faulty component of the DIMM needs a replacement.
UnitInvalidTypeError	memory.Unit	Critical	The memory unit type is invalid.	Create a `show tech-support file` and contact Cisco TAC to see if the failed DIMM needs a replacement.
UnitCatErr	processor.Unit	Critical	The processor has encountered a CATERR error. The system event log (SEL) contains events related to the processor's catastrophic error (CATERR) sensor.	Create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
UnitThermtrip	processor.Unit	Critical	The processor has encountered a THERMTRIP error.	1. Review the product specifications to determine the temperature operating range of the server. 2. Verify that the server fans are working properly. 3. Verify that the air flows on the Cisco UCS chassis or rack server are not obstructed. 4. Power off unused blade servers and rack servers. 5. Set the power profiling, power priority of the server, and the power restore state of the system through server Power Policy. 6. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
UnitTemperatureWarning	processor.Unit	Warning	The processor has a warning temperature threshold condition.	1. Verify that the server fans are working properly. 2. Wait for 24 hours to see if the problem resolves itself. 3. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
UnitTemperatureCritical	processor.Unit	Critical	The processor has a critical temperature threshold condition.	1. Verify that the server fans are working properly. 2. Wait for 24 hours to see if the problem resolves itself. 3. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
NodeRiser1Missing	pci.Node	Warning	The PCIe node Riser 1 is missing. No PCIe lanes to CPU1 can be utilized.	1. Review the Cisco UCS X440p PCIe Node Installation and Service Guide. 2. Ensure that all the required hardware are installed as per the guide. 3. If the issue still persists, create a `show tech-support` file and contact Cisco TAC.
NodeRiserMismatch	pci.Node	Warning	The PCIe node Riser type mismatch. Risers will remain powered off.	1. Review the Cisco UCS X440p PCIe Node Installation and Service Guide. 2. Mixing of GPU models are not supported in the compute node. Ensure that each PCIe node is configured with the same type of GPU.

Name	MO	Severity	Explanation	Recommended Action
NodeRiser2PresentCPU2Absent	pci.Node	Warning	PCIe node Riser 2 is present, but CPU2 is absent. PCIe slots on Riser 2 are not connected.	1. Review the Cisco UCS X440p PCIe Node Installation and Service Guide. 2. Ensure that all the required hardware are installed as per the guide. 3. If the issue still persists, create a show tech-support file and contact Cisco TAC.
NodePCIeLinkConfigIssue	pci.Node	Warning	PCIe link or port configuration issue detected. PCIe links may not be up or configured properly between PCIe slots and CPUs.	1. Review the Cisco UCS X440p PCIe Node Installation and Service Guide. 2. Ensure that all the required hardware are installed as per the guide. 3. If the issue still persists, create a show tech-support file and contact Cisco TAC.
NodeRiser1PowerFault	pci.Node	Critical	PCIe node Riser 1 power fault detected.	1. Review the Cisco UCS X440p PCIe Node Installation and Service Guide. 2. Verify that the Power cable for Riser 1 is inserted correctly in the PCIe node. 3. Verify that the Power cable for Riser 1 is connected to the power source.
NodeRiser2PowerFault	pci.Node	Critical	PCIe node Riser 2 power fault detected.	1. Review the Cisco UCS X440p PCIe Node Installation and Service Guide. 2. Verify that the Power cable for Riser 2 is inserted correctly in the PCIe node. 3. Verify that the Power cable for Riser 2 is connected to the power source.
NodePowerFault	pci.Node	Critical	PCIe node power fault detected.	1. Review the Cisco UCS X440p PCIe Node Installation and Service Guide. 2. Verify that the PCIe node has two dark colored GPU cables that carry power and data. 3. Verify that the Power cables are connected to the power source and inserted into the PCIe node.

■ **Server Components Alarms**

Name	MO	Severity	Explanation	Recommended Action
NodeUnsupportedPCIeCardPresentOnRiser1	pci.Node	Warning	PCIe node has an unsupported PCIe card present on Riser 1. Riser will remain powered off.	1. Review the Cisco UCS X210c M6 Compute Node Installation and Service Note and Cisco UCS X440p PCIe Node Installation and Service Guide. 2. Install the recommended type of GPU on Riser 1. 3. Power on the riser.
NodeUnsupportedPCIeCardPresentOnRiser2	pci.Node	Warning	PCIe node has an unsupported PCIe card present on Riser 2. Riser will remain powered off.	1. Review the Cisco UCS X210c M6 Compute Node Installation and Service Note and Cisco UCS X440p PCIe Node Installation and Service Guide. 2. Install the recommended type of GPU on Riser 2. 3. Power on the riser.
NodeUnknownPCIeCardPresentOnRiser1	pci.Node	Warning	PCIe node has an unknown PCIe card present on Riser 1. Riser will remain powered off.	1. Review the Cisco UCS X210c M6 Compute Node Installation and Service Note and Cisco UCS X440p PCIe Node Installation and Service Guide. 2. Install the recommended type of GPU on Riser 1. 3. Power on the riser.
NodeUnknownPCIeCardPresentOnRiser2	pci.Node	Warning	PCIe node has an unknown PCIe card present on Riser 2. Riser will remain powered off.	1. Review the Cisco UCS X210c M6 Compute Node Installation and Service Note and Cisco UCS X440p PCIe Node Installation and Service Guide. 2. Install the recommended type of GPU on Riser 1. 3. Power on the riser.
NodePresentXFM1Absent	pci.Node	Warning	PCIe node detected with missing XFM1. PCIe node cannot be fully managed without both XFMs being present.	1. Review the Cisco UCS X440p PCIe Node Installation and Service Guide. 2. Ensure that all the required hardware are installed as per the guide. 3. If the issue still persists, create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
ControllerLostConfiguration	storage.Controller	Critical	This alarm occurs when the storage controller has lost its configuration data.	When you replace a RAID controller, the RAID configuration that is stored in the controller is lost. Use this procedure to restore your RAID configuration to the new RAID Controller. • For Legacy mode 1. Power off the server, replace your RAID controller. 2. Reboot the server . 3. Press **F** to import foreign configuration(s) when you see the on-screen prompt. • For UEFI Boot mode, 1. Check if the server is configured in Unified Extensible Firmware Interface (UEFI) mode. 2. Power off the server, replace the RAID controller. 3. Reboot the server. 4. Press **F2** when prompted to enter the BIOS Setup utility. 5. Under **Setup Utility**, navigate to **Advanced > Select controller > Configure**, and click Import foreign configuration to Import. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
ControllerFailed	storage.Controller	Critical	This alarm occurs when the storage controller is in failed state.	If the Storage controller is in **failed** state, create a `show tech-support` file and contact Cisco TAC to see if the controller needs replacement.
ControllerFlashDegraded	storage.Controller	Critical	This alarm occurs when the storage controller is functional, but the on-board flash has degraded.	If you see this fault, take the following action: 1. Reset the CIMC and update Board Controller firmware. 2. For PCI and mezz-based controllers, check the seating of the storage controller. If the problem persists, create a `show tech-support` file and contact Cisco TAC to see if the controller needs replacement.

Name	MO	Severity	Explanation	Recommended Action
ControllerFlashFailed	storage.Controller	Critical	This alarm occurs when the storage controller is functional but the on-board flash has failed.	If the flash is in **failed** state, create a `show tech-support` file and contact Cisco TAC to see if the controller needs replacement.
ControllerInvalidFirmware	storage.Controller	Critical	This alarm occurs when the storage controller contains invalid firmware.	1. Update the firmware of the Storage Controller. 2. Reboot the controller. 3. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
ControllerAuthFailure	storage.Controller	Critical	This alarm occurs when SPDM authentication fails for the storage controller.	If you see this fault, take the following actions: 1. Check whether the storage controller is in the list of supported controllers, if not, create a `show tech-support file` and contact Cisco TAC to replace with a supported controller. 2. If the Storage Controller firmware has been updated, reboot the controller.
ControllerInvalidConfiguration	storage.Controller	Critical	This alarm occurs when the storage controller contains invalid configuration.	1. Check whether the storage controller is in the list of supported controllers. 2. If not, create a `show tech-support file` and contact Cisco TAC to replace with a supported controller. 3. If the above actions do not resolve the issue,
ControllerUnresponsive	storage.Controller	Critical	This alarm occurs when contact with the storage controller is probably lost, and the storage controller has become unresponsive.	For PCI and mezz-based storage controllers, check the seating of the storage controller. If the problem persists, create a `show tech-support file` and contact Cisco TAC to see if the controller needs replacement.

Name	MO	Severity	Explanation	Recommended Action
ControllerForeignConfig	storage.Controller	Critical	This alarm occurs when foreign configurations are present in the physical drives attached to the storage controller.	If you see this fault, take the following actions: 1. On the GUI, click **Clear Foreign Configuration** under ellipsis menu by navigating as follows: **Servers>Server Name> Inventory>Storage Controller>Controller Name** 2. If the above actions do not resolve the issue, create a show tech-support file and contact Cisco TAC.
PhysicalDiskFailed	storage.PhysicalDisk	Critical	This alarm occurs when the storage physical disk is in failed state.	If the drive state is in **failed** state, create a show tech-support file and contact Cisco TAC to see if the disk needs to be replaced.
PhysicalDiskPredictiveFailure	storage.PhysicalDisk	Critical	This alarm occurs when storage physical disk is in predictive failure state.	If the drive state is in **predictive-failure** state, create a show tech-support file and contact Cisco TAC to see if the disk needs to be replaced.
PhysicalDiskOffline	storage.PhysicalDisk	Critical	This alarm occurs when storage physical disk is in Offline state.	If you see this fault, take the following actions: 1. Verify the presence and health of physical disks. 2. If applicable, reseat the disks. 3. If the above actions do not resolve the issue, create a show tech-support file and contact Cisco TAC to replace the used disks.
PhysicalDiskUnConfiguredBad	storage.PhysicalDisk	Warning	This alarm occurs when the storage physical disk is in Unconfigured Bad state and is not available for RAID volume.	If you see this fault, take the following actions: 1. Verify the connectivity between physical disks RAID Controller. 2. Verify the presence and health of physical disks. 3. Reseat the disks. 4. If the above actions do not resolve the issue, create a show tech-support file and contact Cisco TAC to see if the used disks need replacement.

Name	MO	Severity	Explanation	Recommended Action
PhysicalDiskForeignConfig	storage.PhysicalDisk	Critical	This alarm occurs when the storage physical disk contains a foreign configuration.	If you see this fault, take the following actions: 1. Review Storage Policy configuration in the service profile and verify that the selected server meets the requirements in the policy. 2. If applicable, reseat the disks. 3. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC to see if the disks need replacement.
PhysicalDiskSelfTestFail	storage.PhysicalDisk	Critical	This alarm occurs when the self-test on a storage physical disk has failed.	Create a `show tech-support file` and contact Cisco TAC.
VirtualDriveDegraded	storage.VirtualDrive	Critical	This alarm occurs when the storage virtual drive is in degraded state.	If you see this fault, take the following actions: 1. If the drive is performing a consistency check operation, wait for the operation to complete. 2. Verify the presence and health of disks that are used by the virtual drive. 3. If applicable, reseat the disks. 4. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC to see if the used disks need to be replaced.
VirtualDrivePartiallyDegraded	storage.VirtualDrive	Critical	The storage virtual drive is partially degraded. The operating condition of the virtual drive is not optimal.	If you see this fault, take the following actions: 1. If the drive is performing a consistency check operation, wait for the operation to complete. 2. Verify the presence and health of disks that are used by the virtual drive. 3. If applicable, reseat the disks. 4. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC to see if the disks need replacement.

Name	MO	Severity	Explanation	Recommended Action
VirtualDriveOffline	storage.VirtualDrive	Critical	This alarm occurs when the storage virtual drive is in offline state.	If you see this fault, take the following actions: 1. Verify the presence and health of disks that are used by the virtual drive. 2. If applicable, reseat the disks. 3. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC to see if the disks need replacement.
RaidBatteryDegraded	storage.BatteryBackupUnit	Critical	This alarm occurs when the storage battery backup unit is in degraded state.	If you see this fault, take the following actions: 1. If the fault reason indicates the backup unit is in a relearning cycle, wait for relearning to complete. 2. If the fault reason indicates the backup unit is about to fail, create a `show tech-support file` and contact Cisco TAC to see if backup unit needs replacement.
FruMissing	equipment.Fru	Critical	This alarm typically occurs when any hardware component is missing in a server, chassis, FEX or FI and the server or chassis is not rediscovered manually.	If you see this fault, take the following actions: 1. Make sure the hardware component is inserted in the correct slot in the server. 2. Check whether the hardware component is connected and configured properly and is running the recommended firmware version. 3. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
FruReplaced	equipment.Fru	Critical	This alarm typically occurs when any adapter is replaced in a server and the server is not decommissioned and recommissioned.	If you see this fault, take the following actions: 1. For rack servers, decommission and recommission the server if any hardware component is changed. 2. For non-rack servers, acknowledge the server if any hardware component is changed. 3. If no hardware component was changed, Create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
RackFanSpeedCritical	equipment.Fan	Critical	The server fan has a speed threshold condition. This fault typically occurs when a fan is running at a speed that is too slow or too fast. A malfunctioning fan can affect the operating temperature of the rack server.	If you see this fault, take the following actions: 1. If the fan is running below the expected speed, ensure that the fan blades are not blocked. 2. If the fan is running above the expected speed, remove and re-insert the fan. 3. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC to see if the fan needs replacement.
RackPsuInputLost	equipment.Psu	Warning	The power supply has no AC input.	1. Monitor the PSU status. 2. Verify that the power cord is properly connected to the power supply and to the power source. 3. If possible, remove and reseat the PSU. 4. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
RackPsuTemperatureCritical	equipment.Psu	Critical	The power supply has a temperature threshold condition.	1. Monitor the PSU status. 2. Verify that the server fans are working properly. 3. Create a `show tech-support` file and contact Cisco TAC to see if the fan needs replacement.
RackPsuTemperatureWarning	equipment.Psu	Warning	The power supply has a temperature threshold condition.	1. Monitor the PSU status. 2. Verify that the server fans are working properly. 3. Create a `show tech-support` file and contact Cisco TAC to see if the faulty fan needs replacement.
RackPsuOutputCurrentCritical	equipment.Psu	Critical	The power supply has a output current threshold condition.	Create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
RackPsuOutputCurrentWarning	equipment.Psu	Warning	The power supply has a output current threshold condition.	Create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
RackPsuOutputVoltageCritical	equipment.Psu	Critical	The power supply has an output voltage threshold condition.	Create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.

Name	MO	Severity	Explanation	Recommended Action
RackPsuOutputVoltageWarning	equipment.Psu	Warning	The power supply has an output voltage threshold condition.	Create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
RackPsuOutputPowerCritical	equipment.Psu	Critical	The server power supply has an output power threshold condition. This fault occurs if the current output of the PSU in the rack server is far above or below the non-recoverable threshold value.	Create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
RackPsuOutputPowerWarning	equipment.Psu	Warning	The server power supply has an output power threshold condition. This fault occurs if the current output of the PSU in the rack server is far above or below the non-recoverable threshold value.	Create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
ServerProfileStateOutOfSyncWarning	server.profile	Warning	The server profile moved to Out-of-sync state.	1. Evaluate the differences between the server profile configuration and the end-point configuration. 2. Redeploy server profile to apply the configuration in server profile.
ServerProfileStatePendingChangesWarning	server.profile	Warning	The server profile has moved to pending-changes state.	Check the server policy configuration for Pending-changes and deploy the server profile again to apply the changes.
ComputeCimcFirmwareNotSupported	compute.BladeIdentity	Warning	This fault indicates that one of the IO modules is missing.	Intersight Managed Mode does not support the existing firmware version. Upgrade the server using the firmware upgrade option in the Chassis tab.
ComputeServerNotConnected	compute.BladeIdentity	Warning	Server discovery failed because the device is not connected.	Server discovery failed because the device is not connected. For further assistance, contact Cisco TAC.
ComputeServerDisconnected	compute.Physical	Warning	Server is not reachable.	If you see this alarm, take the following actions. Check the server's network connectivity.

Name	MO	Severity	Explanation	Recommended Action
ComputePhysicalBiosPostTimeOut	compute.Physical	Critical	This alarm typically occurs when the server has encountered a BIOS POST timeout.	For further assistance, contact Cisco TAC.
StoragePhysicalDiskReadyForRemoval	storage.PhysicalDisk	Informational (Info)	The physical disk is in quiesced state and ready for removal.	For further assistance, contact Cisco TAC.
StoragePhysicalDiskRebuilding	storage.PhysicalDisk	Informational (Info)	The physical disk is in rebuilding state.	For further assistance, contact Cisco TAC.
StorageVirtualDriveCacheDegraded	storage.VirtualDrive	Warning	Virtual drive cache is in degraded state.	For further assistance, contact Cisco TAC.